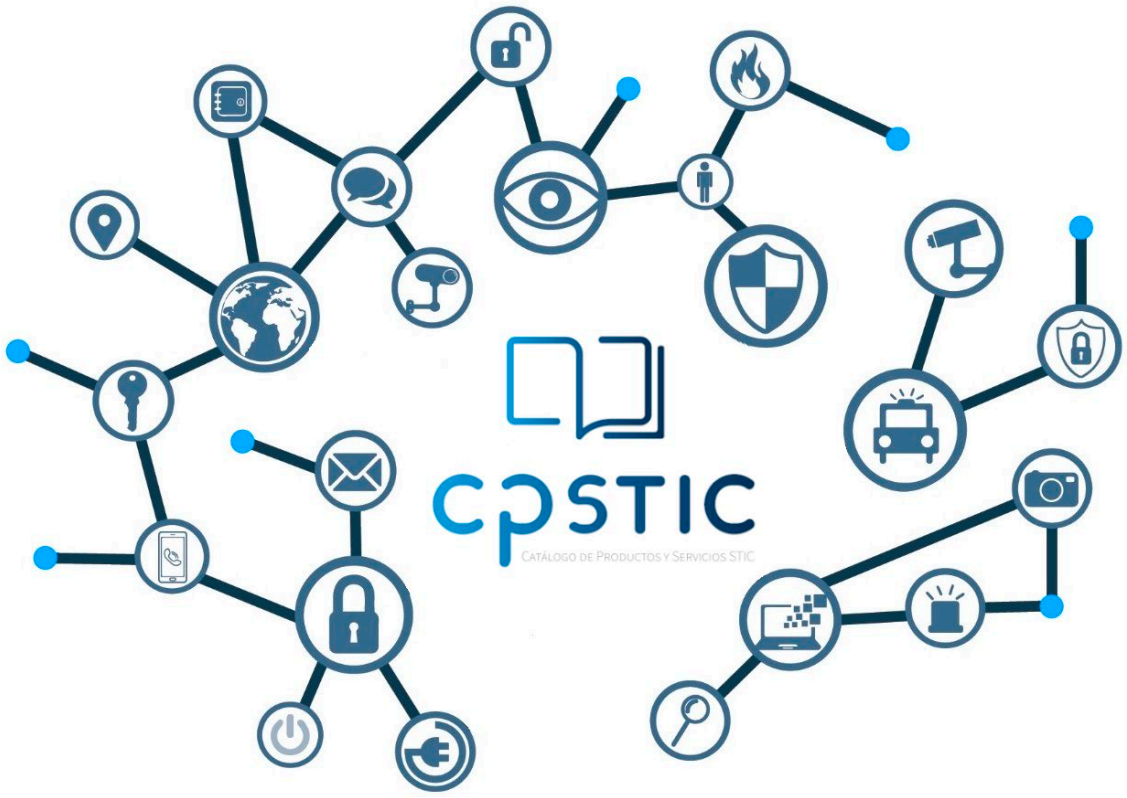
centro criptológico nacional

Guía de Seguridad de las TIC
CCN-STIC 1225

Procedimiento de Empleo Seguro
SPLUNK



Julio 2023

MINISTERIO DE DEFENSA

Catálogo de Publicaciones de la Administración General del Estado
https://cpage.mpr.gob.es

Edita:

MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA

CCN centro criptológico nacional

CENTRO CRIPTOLOGICO NACIONAL
cn=CENTRO CRIPTOLOGICO NACIONAL, 2.5.4.97=VATES-S2800155J, ou=CENTRO CRIPTOLOGICO NACIONAL, o=CENTRO CRIPTOLOGICO NACIONAL, c=ES
2024.01.30 10:04:16 +01'00'

Pº de la Castellana 109, 28046 Madrid

NIPO: 083-24-015-0.
Fecha de Edición: enero de 2024

LIMITACIÓN DE RESPONSABILIDAD

El presente documento se proporciona de acuerdo con los términos en él recogidos, rechazando expresamente cualquier tipo de garantía implícita que se pueda encontrar relacionada. En ningún caso, el Centro Criptológico Nacional puede ser considerado responsable del daño directo, indirecto, fortuito o extraordinario derivado de la utilización de la información y software que se indican incluso cuando se advierta de tal posibilidad.

AVISO LEGAL

ÍNDICE

1. INTRODUCCIÓN

1. Splunk Enterprise es una plataforma de gestión de eventos e información de seguridad (SIEM) que proporciona una visibilidad completa de la postura de seguridad.
2. Splunk Enterprise permite gestionar el ciclo completo en una organización, incluyendo capacidades de Detección, Monitorización, Investigación y Respuesta ante incidentes de Seguridad. Incorpora capacidades de búsqueda y generación de informes sin precedentes, análisis avanzados, inteligencia artificial integrada y contenido de seguridad predefinido y dinámico para acelerar la detección e investigación de amenazas.
3. Splunk permite clasificar por prioridad los incidentes, priorizando los incidentes que afecten a activos o identidades críticos. Permite generar alertas basadas en riesgo, identificando anomalías y amenazas tanto externas como internas. Las más de 2500 reglas de detección abarcan todos los ámbitos de seguridad: IT, OT, IoT, IoMT y las nubes públicas en cualquiera de sus formatos.
4. Algunas de sus características principales son:

    - Indexación: Splunk Enterprise puede recopilar datos de dispositivos y aplicaciones como sitios web, servidores, bases de datos, sistemas operativos y más. Una vez que se recopilan los datos, el índice segmenta, almacena, comprime los datos y mantiene los metadatos de apoyo para acelerar la búsqueda.
    - Búsquedas: La búsqueda es la forma principal en que los usuarios navegan por sus datos en Splunk Enterprise. Puede guardar una búsqueda como informe y utilizarla para potenciar los *dashboard panels*.
    - Alertas: Las alertas le notifican cuando los resultados de búsqueda, tanto históricos como en tiempo real, cumplen las condiciones configuradas. Puede configurar alertas para desencadenar acciones.
    - *Dashboards*: Los paneles del tablero generalmente están conectados a búsquedas guardadas o pivotes. Muestran los resultados de búsquedas completadas y datos de búsquedas en tiempo real que se ejecutan en segundo plano.
    - Informes: Splunk Enterprise le permite guardar búsquedas y pivotes como informes y luego agregar informes a los tableros como paneles de tablero.
    - Modelo de datos: Los modelos de datos codifican conocimiento de dominio especializado sobre uno o más conjuntos de datos indexados. Permiten a los usuarios de *Pivot Editor* crear informes y paneles sin diseñar las búsquedas que los generan.

2. OBJETO Y ALCANCE

5. El objeto del presente documento es servir como guía para **realizar una instalación y configuración segura de la solución Splunk Enterprise 8.2.**

6. **Este producto se sitúa dentro de la Familia de Sistemas de Gestión de Eventos de Seguridad de la tipología definida por el CCN (CPSTIC).**

   NOTA: algunas configuraciones o guías referenciadas en el presente documento provienen de versiones anteriores a la 8.2 debido a que no ha habido cambios en el proceso de implementación y configuración del producto respecto a dichas versiones.

3. ORGANIZACIÓN DEL DOCUMENTO

7. Este documento se compone de los siguientes apartados:

- Apartado **4**. En este apartado se recogen aspectos y recomendaciones a considerar, antes de proceder a la instalación del producto.
- Apartado **5**. En este apartado se recogen recomendaciones a tener en cuenta durante la fase de instalación del producto.
- Apartado **6**. En este apartado se recogen las configuraciones necesarias para emplear el producto de forma segura.
- Apartado **7**. En este apartado se recogen las tareas recomendadas para la fase de operación o mantenimiento del producto.
- Apartado **8**: Checklist de las tareas a realizar y el estado de cada una de ellas.
- Apartado **9**: Referencias usadas en este documento.
- Apartado **10**: Abreviaturas usadas en este documento.

4. FASE PREVIA A LA INSTALACIÓN

4.1 ENTREGA SEGURA DEL PRODUCTO

8. Splunk Enterprise es un producto *software* y la descarga de este se realiza a través de la propia web de Splunk (enlace de descarga *Splunk Enterprise – REF1)*, se debe registrar en la web de Splunk antes de poder descargar la versión del producto.
9. **Se debe comprobar la integridad de los archivos de la instalación de Splunk**. Para ello, se proporciona un hash MD5 y un hash SHA512. Sin embargo, para una verificación segura, **se debe utilizar el hash SHA-512**. La comprobación se debe llevar a cabo siguiendo estos pasos:
    - Descargar el archivo de instalación de Splunk.
    - Generar el hash SHA-512 del archivo.
    - Comparar con el hash SHA-512 facilitado por Splunk y verificar que coinciden.

4.2 ENTORNO DE INSTALACIÓN SEGURO

10. El entorno físico donde opera el producto debe asegurar que **todos los componentes estén protegidos de cualquier ataque físico**, por lo que se recomienda instalar el *software* en un Centro de Proceso de Datos que cuente con un sistema de control de acceso limitado y restringido al conjunto de personas expresamente autorizadas y protegido contra cualquier amenaza de origen físico.

4.3 REGISTRO Y LICENCIAS

11. El producto requiere la instalación de licencias de uso para su correcto funcionamiento. Existen distintos tipos de licencias disponibles, el detalle de licenciamiento del producto se puede consultar en el apartado *Configure Splunk licenses* de la guía *Splunk-8.2.4-Admin – REF3*.

4.4 CONSIDERACIONES PREVIAS

12. Las consideraciones previas a una instalación del producto se pueden consultar en el documento *Splunk-8.2.4-Installation – REF4* sección *Plan your Splunk Enterprise installation.*
13. Adicionalmente Splunk posee públicamente un documento que contempla todas las arquitecturas soportadas, donde se describe los elementos a tener en cuenta y sus funcionalidades. Ver documento *Splunk-8.2.4-Architectures – REF5*.

4.5 COMPONENTES DEL ENTORNO DE OPERACIÓN

14. En el documento**¡Error! No se encuentra el origen de la referencia.** se pueden ver todos los elementos y distribuciones soportadas por la arquitectura del producto.
15. A modo general Splunk Enterprise consta de los siguientes componentes:
    - Fuente de datos externo de confianza: Fuente de datos externa para transmitir datos no relacionados con el producto al indexador del producto para alimentar

el *datastore* de Splunk. La fuente de datos externa **debe utilizar HTTPS/TLS para comunicarse con el producto**.

- Recolector externo de datos de confianza: Fuente de datos externo para recibir datos no relacionados con producto desde el reenviador del producto para alimentar el almacén de datos de Splunk. La fuente de datos externa **debe utilizar HTTPS/TLS para comunicarse con el producto**.
- Plataforma Host: Un ordenador de propósito general en el que está instalado el sistema operativo Linux y el producto. El producto requiere recursos de red de la plataforma host.
- Estación de trabajo de gestión: Cualquier ordenador de propósito general utilizado por un administrador de seguridad para gestionar el producto de forma remota a través de un navegador web. Tener en cuenta que la plataforma host también puede utilizarse para administrar el producto localmente.
- Servidor SMTP: Servidor de correo electrónico que puede recibir alertas del producto y enviarlas a los usuarios del entorno operativo por correo electrónico.
- Punto de distribución CRL: Servidor que proporciona listas de revocación actualizadas para la funcionalidad de validación de certificados del producto.

5. FASE DE INSTALACIÓN

16. En este apartado se describe cómo llevar a cabo la instalación de Splunk Enterprise en modo seguro.

17. Se debe llevar a cabo la instalación de Splunk Enterprise en la siguiente plataforma:

    - Red Hat Enterprise Linux Server versión 6.5 (Santiago).
    - Arquitectura x86_64 (chequeado en Intel(R) Xeon(R) CPU E3-1220 v3).
    - Security-Enhanced Linux (SELInux) con versión 24 de políticas.

5.1.1 PREREQUISITOS

18. El producto requiere llevar a cabo ciertas acciones previas a la instalación para **asegurar una instalación con parámetros seguros.** El detalle de dichas acciones se puede consultar en el documento *Securing Splunk Enterprise with Common Criteria 7.3.4. Version – REF6.* A continuación, se indican aquellas acciones de vital importancia:

    - Disponer de una suscripción de Red Hat habilitada y configurada.
    - **SELinux debe estar en modo Enforcing** con la política seleccionada en ejecución y la versión 24 de la política. Para ello:
        - Abrir el archivo */etc/selinux/config* y asegurarse de que el valor *SELINUX=enforcing*.
        - Ejecutar *getenforce* y verificar que el resultado sea *enforced*. En caso de que no aparezca el modo *Enforcing*, ejecutar el comando *setenforce 1*.
        - Abrir el archivo de configuración de GRUB */etc/grub.conf*. Asegurarse de que no hay ninguna línea relacionada con SELinux en este fichero. En caso de encontrar alguna línea, se debería de borrar para que el *kernel* no deshabilite el uso de SELinux.
    - Asegurar que la versión de Python es la 2.6.6. Para ello ejecutar el comando:

      /user/bin/python --version
    - Asegurar de que GNOME keyring y las dependencias de Python están instaladas. Para ello ejecutar los comandos:

      yum install gnome-keyring-devel
      yum install gnome-python2-gnomekeyring
    - El paquete *RdRan-2.0.0-1.el6.x86_64.rpm* debe estar instalado.
    - Se deben cifrar los discos duros empleando AES-256 donde se almacene la información de Splunk. Para ello ejecutar los siguientes comandos:

      cryptsetup -c aes-xts-plain64:sha256 –key-size 512 luksFormat /dev/sdb
      cryptsetup -c aes-xts-plain64:sha256 –key-size 512 luksFormat /dev/sdc
      cryptsetup luksOpen /dev/sdb optetc
      cryptsetup luksOpen /dev/sdc opt
      cryptsetup -v status optetc
      cryptsetup -v status opt
      mkfs.ext4 /dev/mapper/optetc
      mkfs.ext4 /dev/mapper/opt

```
mount /dev/mapper/optetc /etc/opt
mount /dev/mapper/opt /opt
chcon -u system_u -r object_r -t usr_t /opt
chcon -u system_u -r object_r -t etc_t /etc/opt
dd if=/dev/urandom of=/root/keyfile bs=1024 count=4
cryptsetup luksAddKey /dev/sdb /root/keyfile
cryptsetup luksAddKey /dev/sdc /root/keyfile
echo "optetc /dev/sdb /root/keyfile luks" >> /etc/crypttab
echo "opt /dev/sdc /root/keyfile luks" >> /etc/crypttab
echo "/dev/mapper/opt /opt ext4 defaults 1 2" >> /etc/fstab
echo "/dev/mapper/optetc /etc/opt ext4 defaults 1 2" >> /etc/fstab
```

- Se debe disponer del paquete RPM que contenga la configuración de seguridad de SELinux para operar en modo seguro. Este paquete estaría disponible en el siguiente enlace. En caso de no estar disponible el fichero en el sitio web, se deberá solicitar al fabricante para su implementación.
- Se debe disponer de los certificados correspondientes para el uso del producto de forma segura. Dichos certificados se pueden consultar en el apartado 6.7 GESTIÓN DE CERTIFICADOS.

5.1.2 INSTALACIÓN

19. Para llevar a cabo la instalación del producto tras su descarga segura (ver apartado 4.1 ENTREGA SEGURA DEL PRODUCTO), se deben llevar a cabo los siguientes pasos:
    - Instalar Splunk 7.3.0 con permisos de usuario root:

      rpm -i splunk-7.3.0-<xxxxxxxxxxxx>-linux-2.6-x86_64.rpm --nodeps
    - Mover los ficheros de configuración de la ubicación por defecto a /etc/opt/splunk.
    - Se deberán generar las claves criptográficas para las comunicaciones del producto:
        - Claves pública y privada para las comunicaciones de auditoría, empleando AES256 y una longitud de clave de, al menos, 3072 bits:

          openssl genrsa -aes256 -out $SPLUNK_ETC/auth/audit/private.pem 3072
          openssl rsa -in $SPLUNK_ETC/auth/audit/private.pem -out $SPLUNK_ETC/auth/audit/public.pem -outform PEM -pubout
        - Claves pública y privada para distServerKeys, empleando AES256 y una longitud de clave de, al menos, 3072 bits:

          openssl genrsa -aes256 -out $SPLUNK_ETC/auth/distServerKeys/private.pem 3072
          openssl rsa -in $SPLUNK_ETC/auth/distServerKeys/private.pem -out $SPLUNK_ETC/auth/distServerKeys/trusted.pem -outform PEM -pubout
    - Descargar el fichero *Splunk SElinux.rpm* desde la página web de Splunk e instalarlo:

      yum install splunk-selinux-<version>.rpm
    - Se solicitará la contraseña para el usuario de gestión *admin*. Introducir la contraseña deseada, la cual deberá cumplir con la política de contraseñas (ver apartado 6.4.2 CONFIGURACIÓN DE ADMINISTRADORES).

6. FASE DE CONFIGURACIÓN

6.1 MODO DE OPERACIÓN SEGURO

20. **Se debe emplear el producto en el modo de operación seguro**. Para ello se debe activar el modo seguro, incluyendo las siguientes modificaciones en el archivo de configuración */etc/opt/splunk/splunk-launch.conf*:

```
SPLUNK_COMMON_CRITERIA=1
SPLUNK_FIPS=1
# Do not generate python byte code
PYTHONDONTWRITEBYTECODE=1
```

6.1.1 PROTECCIÓN DE LA INFORMACIÓN

21. **Se deberá configurar el entorno de ejecución del producto para proteger la información en reposo mediante el cifrado de los datos**, (para más información, consultar el documento *Configuring Splunk Enterprise for Common Criteria 8.1.1– REF10*). Para ello, se deben seguir los siguientes pasos:

    - Iniciar el proceso *dbus*:

      /home/splunk/run_dbus.sh

    - Ejecutar *source /home/splunk/.bashrc* para asegurar que se establezcan las variables de entorno.

    - Inicializar la contraseña del "almacenamiento secreto":

      runcon -u system_u -t splunk_t -r system_r splunk secret-storage --unlock

    - Ver la lisa de claves disponibles:

      runcon -u system_u -t splunk_t -r system_r splunk secret-storage -–spec

    - Para añadir claves al Keyring de GNOME, emplear el siguiente comando:

      runcon -u system_u -t splunk_t -r system_r splunk secret-storage --write --no-prompt <conf-file> <stanza-name> <attribute-name> <passphrase>

6.2 AUTENTICACIÓN

22. **Se deberá llevar a cabo la correcta configuración de los certificados, ya que estos serán empleados para la autenticación interna de los distintos componentes del producto**. Dicha configuración se puede consultar en el apartado 6.7 GESTIÓN DE CERTIFICADOS.

23. Para permitir que un usuario acceda a los servicios y recursos ofrecidos por Splunk, el producto dispone de distintos esquemas de autenticación (para más información, consultar el documento *Splunk-8.2.4-Security – REF2*). Cabe destacar que, para que la autenticación sea efectiva, es necesario que exista una licencia activa.

    - Autenticación local de Splunk mediante usuario y contraseña. Es el esquema por defecto y tiene prioridad sobre cualquier esquema de autenticación externo.

    - LDAP. Soporta la autenticación con sus servicios de autenticación internos o con tu servidor LDAP existente.

- SAML. Soporta el contacto con un IdP que utilice SAML en su versión 2.0 y recuperar la información del usuario que puede asignarse a roles de Splunk.
- Multi-factor. Permite el uso de dos o más servicios de autenticación e incluye la capacidad de utilizar *Duo* o *RSA Manager*.
- *Scripted Authentication API*. Permite el uso de autenticación mediante script para integrar la autenticación de Splunk con un sistema de autenticación externo como RADIUS o PAM.
- Autenticación con *JWT Tokens*.
- Autenticación mediante un *proxy single sign-on*.
- Autenticación mediante un reverse proxy single sing-on.

24. El método de autenticación deseado se seleccionará durante la creación de usuarios. Ver apartado 6.4.2 CONFIGURACIÓN DE ADMINISTRADORES.

6.3 SERVIDORES DE AUTENTICACIÓN

25. En el documento *Splunk-8.2.4-Security – REF2* se puede consultar el detalle de configuración de los distintos servidores de autenticación externos soportados por Splunk. Se dispone de los siguientes:

    - Autenticación LDAP, descrita en la sección *Use LDAP as an authentication scheme.* En caso de emplear LDAP, se deberán activar y configurar los siguientes parámetros para asegurar el empleo de TLS en la autenticación de usuarios.
        - En el servidor:

          TLSCACertificateFile <filename>, TLSCertificateKeyFile <filename>, TLSCipherSuite <cipher-suite-spec>, TLSRandFile <filename>, TLSEphemeralDHParamFile <filename>, TLSVerifyClient [never | allow | try | demand]

        - En el cliente:

          TLS_KEY <filename>, TLS_RANDFILE <filename>, TLS_REQCERT [never | allow | try | demand].
    - Autenticación SAML, descrita en la sección *Use SAML as an authentication scheme for single sign-on.* Se deberán seguir los pasos indicados en el apartado *Secure SSO with TLS certificates on Splunk Enterprise,* para asegurar las operaciones SSO mediante TLS.
    - Autenticacion multifactor, descrita en la sección *Use multi-factor authentication in Splunk Enterprise as an authentication scheme.*
    - Autenticación usando Tokens, descrita en la sección *Authenticate into the Splunk platform with tokens*.
    - Autenticación usando *ProxySSO*, descrita en la sección *Authenticate into the Splunk platform using proxy single sign-on.*
    - Autenticación usando SSO con un reverse *proxy*, descrita en la sección *Authenticate into Splunk Enterprise using single sign-on with reverse proxy.*

- Autenticación usando scripts (PAM, RADIUS) descrita en la sección *Authenticate into Splunk Enterprise using scripts*.

6.4 ADMINISTRACIÓN DEL PRODUCTO

6.4.1 ADMINISTRACIÓN LOCAL Y REMOTA

26. El producto dispone de las siguientes interfaces de administración:
    - Administración remota de tipo GUI, mediante acceso web. Este acceso web se realizará de forma segura mediante el uso de TLS 1.2, ver el apartado 6.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS.
    - Mediante el uso de los archivos de configuración alojados en el directorio de instalación de Splunk, descritos en el apartado 6.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS. Esta administración puede ser vía remota usando SSHv2 o local desde la propia consola del sistema operativo.
    - Administración local y remota (empleando SSHv2) por consola de tipo CLI. La sintaxis que se debe seguir para hacer uso de la consola CLI es la siguiente:

      /splunk <command> [<object>] [[-<parameter>] <value>]

27. **Se recomienda emplear la administración remota de tipo GUI o la administración de tipo CLI para gestionar y configurar el producto.**

6.4.2 CONFIGURACIÓN DE ADMINISTRADORES

28. El producto dispone de los siguientes roles predeterminados:
    - *Admin:* dispone de todos los permisos.
    - *Power:* permite editar todos los objetos compartidos y alertas.
    - *User:* permite crear, editar y ejecutar búsquedas.
    - *SC_admin:* se emplea para crear otros usuarios y roles, pero no dispone de otros permisos administrativos.
29. Sin embargo, permite la creación de roles personalizados, pudiendo configurar así los permisos específicos de los distintos usuarios. Esto se puede realizar modificando el fichero *authorize.conf* desde la interfaz CLI o en la interfaz GUI desde *Settings > Roles.*
30. Durante la creación de usuarios se deberán especificar su rol y el método de autenticación (parámetro *Authentication system*). Al crear un usuario se le asigna una contraseña, por lo que se deberá activar el parámetro *Require password to change on first login*, de tal forma que deba modificarse la contraseña al acceder por primera vez. Todas las contraseñas deberán cumplir con la política de contraseñas definida a continuación.
31. **Se deberá configurar el tiempo de inactividad de las sesiones de los usuarios en cinco (5) minutos**. Para ello se debe modificar el archivo de configuración *authentication.conf* y asignar el valor *timeout* a 300.
32. El detalle de creación y configuración de usuarios y roles se puede consultar en el apartado "*Manage users and roles"* de la guía *Splunk-8.2.4-Security – REF2*.

33. **Se deberá configurar la Política segura de contraseñas**. Para ello desde Spunk Web ir a *Settings > Password Management*. Deberán configurarse los siguientes parámetros:
    - *Minimum Characters:* longitud mínima de la contraseña de doce (12) caracteres.
    - *Numeral:* número de dígitos requeridos de, al menos, 1.
    - *Lowercase:* número de minúsculas requeridas de, al menos, 1.
    - *Uppercase:* número de mayúsculas requeridas de, al menos, 1.
    - *Special Character:* número de caracteres especiales requeridos de, al menos, 1.
    - Marcar la opción **Force existing users to change weak passwords** para obligar a los usuarios existentes a modificar las contraseñas en caso de no cumplir con la política definida.
    - Habilitar el campo History y asignar el campo Password History Count a un valor igual a 5 o superior, para prevenir el uso de las últimas 5 contraseñas.
    - Activar la casilla *Expiration* para forzar a los usuarios a cambiar las contraseñas tras un tiempo definido en el parámetro *Days until password expires:* asignar un valor de 60 o inferior.
    - Activar la casilla *Lockout* para permitir el bloqueo de cuentas. Asignar el campo *Failed login attemps* a un valor de 3 o inferior. Tras el número de fallos de autenticación definidos se bloqueará la cuenta.
    - Asignar el campo *Lockout duration in minutes* a un valor de 5 o superior, para definir el tiempo de bloqueo.
34. Por último, el administrador deberá definir de forma procedural el número de días que deben transcurrir tras el cambio de una contraseña antes de poder modificarla de nuevo en diez (10) días.

6.5 CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS

35. En el documento *Splunk-8.2.4-Security – REF2* se describe la configuración de interfaces, puertos y servicios de forma segura de Splunk Enterprise en la sección *Install Splunk Enterprise Securely > Secure Splunk Enterprise on your network.*
36. Se recomienda deshabilitar aquellos componentes de Splunk que no vayan a ser utilizados para reducir el número de ataques potenciales, se puede consultar el detalle en el apartado *Disable unnecessary Splunk Enterprise components* del documento *Splunk-8.2.4-Security – REF2:*
    - Deshabilitar componentes innecesarios de Splunk Enterprise en implementaciones de Splunk Enterprise de un solo servidor:
        - Si es posible, no ejecutar Splunk Web en reenviadores de ningún tipo.
        - Si es posible, deshabilitar cualquier configuración que permita a los reenviadores recibir datos en puertos de red TCP o UDP o desde otras instancias de Splunk Enterprise.
    - Deshabilitar componentes innecesarios de Splunk Enterprise en implementaciones de Splunk Enterprise de múltiples servidores:

- Si es posible, deshabilitar cualquier configuración que permita que los *Search heads* reciban datos en puertos de red TCP o UDP o desde otras instancias de Splunk Enterprise.
- Si los usuarios no inician sesión en Splunk Web en los *indexers* en un entorno distribuido, desactivar Splunk Web en esos *indexers*.

- En una instalación distribuida con varios servidores, se puede deshabilitar Splunk Web en aquellos servidores donde no se emplee, siguiendo los siguientes pasos:
  - En la barra del sistema, seleccionar *Setting > Server Settings*.
  - Seleccionar General Settings.
  - En la sección *Splunk Web*, en el botón *Run Splunk Web*, seleccionar *No*.
  - Hacer clic en *Save*.
  - Reiniciar la instancia de Splunk Enterprise.

6.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS

37. **Se debe realizar una configuración segura de TLS**. Este proceso es detallado en la sección *About TLS encryption and cipher suites* del documento **¡Error! No se encuentra el origen de la referencia.**:
    - Acudir al directorio */etc/opt/splunk/system/local* dónde se ubican los ficheros de configuración.
    - En los archivos *server.conf, web.conf, outputs.conf, inputs.conf* y *alerts_actions.conf* editar las siguientes líneas de código para emplear únicamente ciphersuites seguras y la versión 1.2 de TLS:

      cipherSuite= ECDHE-ECDSA-AES256-GCM-SHA384:ECDHE-ECDSA-AES128-GCM-SHA256:ECDHE-ECDSA-AES256-SHA384
      sslVersions = tls1.2
    - En el archivo *authentication.conf*, editar la siguiente línea de código:

      [secrets]
      disabled = false
    - Guardar la configuración y cerrar los ficheros.
    - Reiniciar Splunk Enterprise para que los cambios tomen efecto.
38. **Se debe configurar el producto para evitar el empleo de HTTP en las comunicaciones con el servidor web y emplear únicamente HTTPS**:
    - Abrir el fichero de configuración *web.conf*.
    - En *settings*, asignar un puerto http y asignar *SplunkWebSSL* a *true*.

      [settings]
      httpport = <https port number>
      enableSplunkWebSSL = true
    - Reiniciar Splunk Enterprise.
    - Tras reiniciar, para acceder a la instancia de Splunk Web utilizar https://<your site name>:<port>.

39. La configuración del protocolo SSH la lleva a cabo el sistema operativo donde reside el producto, en este caso, el sistema operativo Red Hat. **Se debe asegurar que se utiliza únicamente SSHv2**.

6.7 GESTIÓN DE CERTIFICADOS

40. El detalle de configuración de los certificados se puede consultar en el apartado *Appendix A: How to obtain SSL certificates* de la guía *Splunk-8.2.4-Security – REF2*.

41. El producto emplea los certificados para asegurar las comunicaciones entre los siguientes componentes:

    - Comunicaciones entre el navegador web y el servidor web de Splunk para la gestión remota.
    - Comunicaciones entre los componentes internos del producto (*forwarder* e *indexer*).
    - Comunicaciones entre el producto y el servidor SMTP.

42. Se deberán seguir los siguientes pasos generales:

    - Importar el certificado de la CA que se utilizará para generar el certificado de servidor.
    - Crear un CSR (*Certificate Signing Request*). Se deberá utilizar uno de los siguientes parámetros para la creación del certificado:
        - Tipo de clave ECDSA, con un tamaño de 256 o 384 bits y algoritmo de firma SHA-384 o SHA-256.
    - Importar el certificado de servidor una vez recibido.

6.8 SINCRONIZACIÓN

43. Se recomienda que todos los sistemas utilizados por la organización se encuentren sincronizados para permitir una alta fiabilidad en los sistemas de auditoría y *logging*. **El producto recibe la hora del sistema operativo sobre el que se encuentre desplegado**.

6.9 ACTUALIZACIONES

44. Las actualizaciones del producto deberán llevarse a cabo manualmente por un usuario administrador. Para ello, se deberán seguir los siguientes pasos:

    - Hacer clic en *Update URL* en la consola de gestión web.
    - Autenticarse en el portal de descargas y descargar manualmente el paquete .rpm.
    - Con permisos de administrador, ejecutar el comando *rpm -K <filename.rpm>* para verificar la autenticidad de la descarga empleando la clave pública de Splunk.
    - Realizar la instalación del paquete con el comando *rpm -i fichero_descargado –nodeps,*

6.10 AUTO-CHEQUEOS

45. En el documento *Splunk-8.2.4-Admin – REF3* sección *Check the integrity of your Splunk software files*, se describen los distintos procedimientos para verificar la integridad del producto.

46. Splunk ofrece la capacidad validar los archivos y detectar si ha habido alguna modificación no válida en el software de la plataforma. Esta comprobación se realiza automáticamente en el arranque y también puede llevarse a cabo de forma manual. Se mostrarán los resultados en la consola de monitorización, el detalle se puede consultar en el documento *Splunk-8.2.4-Admin – REF3,* en el apartado *Access and customize health checky.*

47. Para llevar a cabo una validación manual, emplear el siguiente comando desde el directorio de instalación *./splunk validate files*. Esta comprobación manual se puede ejecutar con dos controles adicionales:

    - Es posible especificar el archivo mediante la descripción del archivo correcto utilizando la opción *-manifest* (es válido cualquier archivo *manifest* que se encuentre disponible).
    - Se puede limitar el test a archivos que terminen con *.conf* utilizando la opción *-type conf*.

48. En cuanto a la validación automática, esta se lleva a cabo en dos etapas:

    - Antes de iniciar el servicio *splunkd*, se lleva a cabo una validación preliminar. Esta validación solamente abarca los archivos de configuración por defecto y se muestra un mensaje en la terminal como resultado.
    - Una vez iniciado *splunkd*, el test de validación verifica todos los archivos proporcionados por Splunk Enterprise, incluyendo archivos de configuración, librerías, binarios, y archivos de datos. Los resultados se guardan en el archivo *splunkd.log*, y también se muestran los mensajes del boletín del sistema en la interfaz web de Splunk. La segunda etapa de la validación puede ser configurada en el archivo *limits.conf*.

49. La lectura de todos los archivos proporcionados con la instalación tiene un efecto moderado en el rendimiento de E/S. Si necesita reiniciar Splunk varias veces en un corto periodo de tiempo, es posible que sea necesario desactivar esta comprobación temporalmente para mejorar el rendimiento de E/ S.

50. Los archivos se validan contra el archivo *manifest* en el directorio de instalación. Si este archivo se elimina o altera, la comprobación puede no funcionar correctamente.

51. En caso de fallo en la validación de los archivos, el servicio no se iniciará indicando el error en el archivo *splunkd.log*.

6.11 ALTA DISPONIBILIDAD

52. Splunk Enterprise emplea clusterización para proporcionar alta disponibilidad, esta puede ser aplicada no solo a la capa de indexado sino también a la capa de gestión y búsqueda. El detalle se puede consultar en el documento *Splunk-8.2.4-Deploy – REF7* sección *High availability deployment: Indexer cluster*.

53. En el documento *Splunk-8.2.4-Architectures – REF5* se pueden ver los modelos y arquitecturas soportadas por Splunk Enterprise y las capacidades que proporcionan cada uno de estos.
54. En el documento *Splunk-8.2.4-Indexer Cluster – REF9* se describe la instalación de un entorno de alta disponibilidad. Los pasos para implementarlo son los siguientes:
    - Instalar las instancias necesarias de Splunk Enterprise siguiendo el procedimiento de instalación seguro de esta guía.
    - Desplegar el *cluster* de indexadores según lo indicado en el siguiente enlace. No ha de aplicarse ningún parámetro específico de seguridad.
    - Si se desea, implementar un clúster de servidores de búsqueda consultar el siguiente enlace.
    - Configurar la licencia de Splunk Enterprise.
    - Conectar los nodos pares a las fuentes de datos.

6.12 AUDITORÍA

6.12.1 REGISTRO DE EVENTOS

55. En el documento *Splunk-8.2.4-Security – REF2* sección *Audit activity in Splunk Enterprise* se describe cómo se realiza el registro de las actividades del producto. El producto registra todos los eventos de seguridad relevantes
56. Dentro de un evento de auditoría se encuentra la siguiente información:
    - Marca de tiempo. Fecha y hora en la que sucedió el evento.
    - Información de usuario. Quien generó el evento (si no tiene información de usuario, Splunk asigna el usuario a quien esté logueado en ese momento).
    - Información adicional. Detalles del evento, éxito/denegado, etc.
57. El producto almacena los registros de auditoría en el fichero *$SPLUNK_HOME/var/og/splunk/audit.log.*
58. Es posible realizar el envío de los registros a un servidor externo empleando TLSv1.2. Para ello es necesario configurar el producto como un *forwarder*, de tal forma que reenviará los registros de auditoría junto al resto de eventos a la ubicación configurada. Se puede consultar el apartado 6.14 FUNCIONES DE SEGURIDAD para ver los pasos de configuración el envío como *forwarder*.
59. Se recomienda configurar el reenvío de los registros a un servidor externo.

6.13 BACKUP

60. **Se recomienda establecer copias de seguridad periódicas**. El producto no dispone de un mecanismo de copias de seguridad, si no que se deberán copiar los archivos y directorios con la configuración del producto. Estos son los siguientes:
    - El directorio *$SPLUNK_HOME/etc/* y sus subdirectorios contienen toda la configuración para la instalación de Splunk, incluidas las búsquedas guardadas,

las cuentas de usuario, las etiquetas y los nombres de tipo de origen personalizados, y todas las aplicaciones.

61. Se recomienda almacenar la copia de seguridad en una ubicación independiente, distinta al dispositivo en el que se despliega el producto.

62. En los siguientes documentos se pueden consultar los procedimientos técnicos detallados para la realización de copias de seguridad de los diferentes componentes de Splunk:

    - En el documento *Splunk-8.2.4-Admin* – REF3 sección *Splunk platform administration: the big picture* se describen las copias recomendadas de los distintos componentes del producto. En la sección Back up and restore KV store se describe cómo hacer copia de seguridad del componente KVStore.
    - El documento *Splunk-8.2.4-DistSearch* – REF8 sección *Back up and archive your indexes* indica cómo realizar las copias de seguridad de los datos indexes.
    - El documento *Splunk-8.2.4-DistSearch* – REF8 sección *Back up and restore search head cluster settings* indica cómo realizar las copias de los datos de *cluster*.

6.14 FUNCIONES DE SEGURIDAD

63. El documento *Splunk-8.2.4-Security – REF2* describe las capacidades de Splunk, así como las consideraciones a tener en cuenta en un despliegue para mantener la plataforma segura.

64. Una de ellas es el envío de eventos a un servidor remoto *syslog* mediante la funcionalidad de *forwarding*. Este ejemplo muestra cómo configurar un *Heavy Forwarder* para enviar datos desde hosts cuyos nombres comienzan con "nyc" a un servidor syslog llamado *loghost.example.com* a través del puerto 514:

    - Editar *props.conf* y *transforms.conf* para especificar los criterios de filtrado.
    - En *props.conf*, aplicar la transformación *send_to_syslog* a todos los nombres de host que comienzan con nyc:

      ```
      [host::nyc*]
      TRANSFORMS-nyc = send_to_syslog
      ```

    - En *transforms.conf*, configurar la transformación *send_to_syslog* para especificar *_SYSLOG_ROUTING* como *DEST_KEY* y el grupo de destino *my_syslog_group* como *FORMAT*:

      ```
      [send_to_syslog]
      REGEX = .
      DEST_KEY = _SYSLOG_ROUTING
      FORMAT = my_syslog_group
      ```

    - En *outputs.conf*, definir el grupo de destino *my_syslog_group* para el servidor no-Splunk:

      ```
      [syslog:my_syslog_group]
      server = loghost.example.com:514
      ```

    - En las configuraciones indicadas en el apartado 6.6 CONFIGURACIÓN DE PROTOCOLOS SEGUROS, se exige el empleo de TLSv1.2 en todas las comunicaciones en las que Splunk actúe como *forwarder*, mediante el fichero *outputs.conf.*

7. FASE DE OPERACIÓN

65. El correcto funcionamiento del producto requiere de unas características que deben estar presentes en el entorno operacional:

    - **El producto debe contar con las últimas actualizaciones de seguridad** para preservar al mismo de amenazas y vulnerabilidades conocidas.
    - **Se deben mantener y analizar los registros de auditoría**. Estos registros estarán protegidos de borrados y modificaciones no autorizadas, y solamente el personal de seguridad autorizado podrá acceder a ellos.
    - **Se deben gestionar correctamente los certificados** utilizados, actualizándolos cuando sea necesario, por ejemplo, al expirar.
    - **Se deben realizar copias de seguridad** de manera periódica.

66. Por otra parte, Splunk Enterprise ofrece dos modelos de monitorización para controlar el correcto uso del producto en fase de operación:

    - Consola de monitorización. Herramienta basada en búsqueda, diseñada para brindar a los usuarios información detallada sobre la topología y el rendimiento de su implementación. Incluye una serie de paneles preconstruidos que ofrecen visibilidad en áreas clave, como el rendimiento de búsqueda e indexación, el uso de recursos, el uso de licencias, etc. Los usuarios pueden aprovechar la Consola de Monitorización para hacer un seguimiento del estado de su implementación, independientemente del tipo de topología utilizada, desde implementaciones de una sola instancia hasta complejos clústeres de indexadores de varios sitios.
    - Componente de monitorización pro-activa. Esta herramienta basada en REST de Splunk permite supervisar el estado de salud de las funcionalidades de una implementación de Splunk Enterprise. La monitorización se lleva a cabo a través de la salida de un punto de conexión REST API. Cada funcionalidad informa su estado de salud mediante una estructura de árbol que proporciona una vista continua y de alto nivel del estado de salud de la implementación. Hay dos opciones para acceder a la información del estado de salud de las funcionalidades. La primera opción es utilizar el informe de salud de splunkd disponible en Splunk Web. La segunda opción es acceder a la información del estado de salud directamente desde el punto de conexión */server/health/splunkd.*

8. CHECKLIST

ACCIONES	SÍ	NO	OBSERVACIONES
DESPLIEGUE E INSTALACIÓN			
Verificación de la integridad de la descarga	☐	☐	
Registro de licencias	☐	☐	
CONFIGURACIÓN			
MODO DE OPERACIÓN SEGURO			
Activación del modo seguro	☐	☐	
Configuración del cifrado de disco	☐	☐	
ADMINISTRACIÓN DEL PRODUCTO			
Configuración de roles y usuarios	☐	☐	
Configuración de la política de contraseñas	☐	☐	
Configuración de los parámetros de sesión	☐	☐	
CONFIGURACIÓN DE INTERFACES, PUERTOS Y SERVICIOS			
Deshabilitar las interfaces y servicios no empleados	☐	☐	
CONFIGURACIÓN DE PROTOCOLOS SEGUROS			
Configuración de TLSv1.2	☐	☐	
Configuración de HTTPS	☐	☐	
Configuración de SSHv2	☐	☐	
GESTIÓN DE CERTIFICADOS			
Importar CA, crear CSR e importar el certificado de servidor	☐	☐	
COPIAS DE SEGURIDAD			
Creación de los backups	☐	☐	
AUDITORÍA			

ACCIONES	SÍ	NO	OBSERVACIONES
Configuración del envío de los logs a un servidor Syslog	☐	☐	

9. REFERENCIAS

REF1 *Splunk Enterprise*
https://www.Splunk.com/en_us/download.html

REF2 *Splunk-8.2.4-Security*
https://docs.splunk.com/Documentation/Splunk/8.2.4/Security/

REF3 *Splunk-8.2.4-Admin*
https://docs.splunk.com/Documentation/Splunk/8.2.4/Admin/

REF4 *Splunk-8.2.4-Installation*
https://docs.splunk.com/Documentation/Splunk/8.2.4/Installation/

REF5 *Splunk-8.2.4-Architectures*
https://www.splunk.com/pdfs/technical-briefs/splunk-validated-architectures.pdf

REF6 *Securing Splunk Enterprise with Common Criteria 7.3.4. Version 30/07/2021*
https://docs.splunk.com/Documentation/Splunk/7.3.4/CommonCriteria/Aboutthismanual

REF7 *Splunk-8.2.4-Deploy*
https://docs.splunk.com/Documentation/Splunk/9.0.4/Deploy/Distributedoverview

REF8 *Splunk-8.2.4-DistSearch*
https://docs.splunk.com/Documentation/Splunk/8.2.4/DistSearch/Whatisdistributedsearch

REF9 *Splunk-8.2.4-Indexer Cluster*
https://docs.splunk.com/Documentation/Splunk/8.2.10/Deploy/Indexercluster

REF10 *Configuring Splunk Enterprise for Common Criteria 8.1.1*
https://docs.splunk.com/Documentation/Splunk/8.1.1/CommonCriteria/Commoncriteriainstallationandconfigurationoverview

10.ABREVIATURAS

CCN	Centro Criptológico Nacional
CLI	*Command Line Interface*
CPSTIC	Catálogo de Productos y Servicios TIC
CPU	*Central Processing Unit*
CRL	*Certificate Revocation List*
ECDSA	*Elliptic Curve Digital Signature Algorithm*
FTP	*File Transfer Protocol*
HTTPS	*Hypertext Transfer Protocol Secure*
IKE	*Internet Key Exchange*
IoMT	*Internet of Medical Things*
IoT	*Internet of Things*
IT	*Information Technology*
LDAP	*Lightweight Directory Access Protocol*
NTP	*Network Time Protocol*
OT	*Operational Technology*
PAM	*Privileged Access Manager*
RSS	*Really Simple Syndication*
SAML	*Security Assertions Markup Language*
SHA	*Secure Hash Algorithm*
SIEM	*Security Information and Event Management*
SMTP	*Simple Mail Transfer Protocol*
SPL	*Search Processing Language*
SSH	*Secure Shell*
SSO	*Single Sign On*
STIC	Servicio de Tecnologías de la Información y Telecomunicaciones
TLS	*Transport Layer Security*
URL	*Uniform Resource Locator*
XSRF	*Cross-Site Request Forgery*
XSS	*Cross-Site Scripting*

PUBLICACIONES DE DEFENSA

GOBIERNO DE ESPAÑA
MINISTERIO DE DEFENSA
SUBSECRETARÍA DE DEFENSA
SECRETARÍA GENERAL TÉCNICA
SUBDIRECCIÓN GENERAL DE PUBLICACIONES Y PATRIMONIO CULTURAL